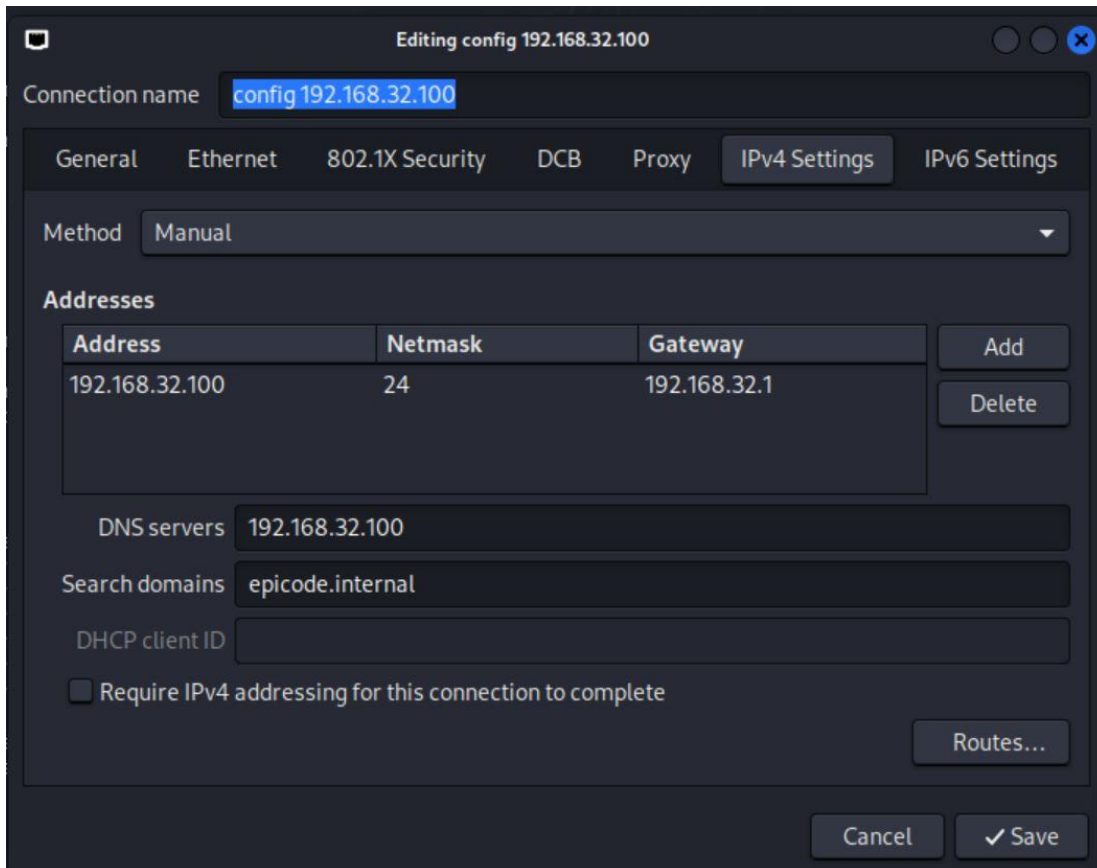
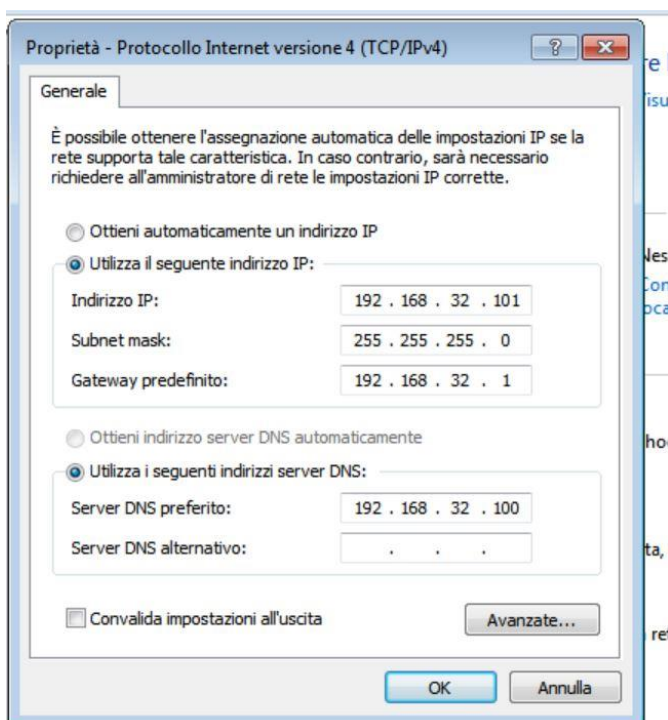


W4D4 ESAME

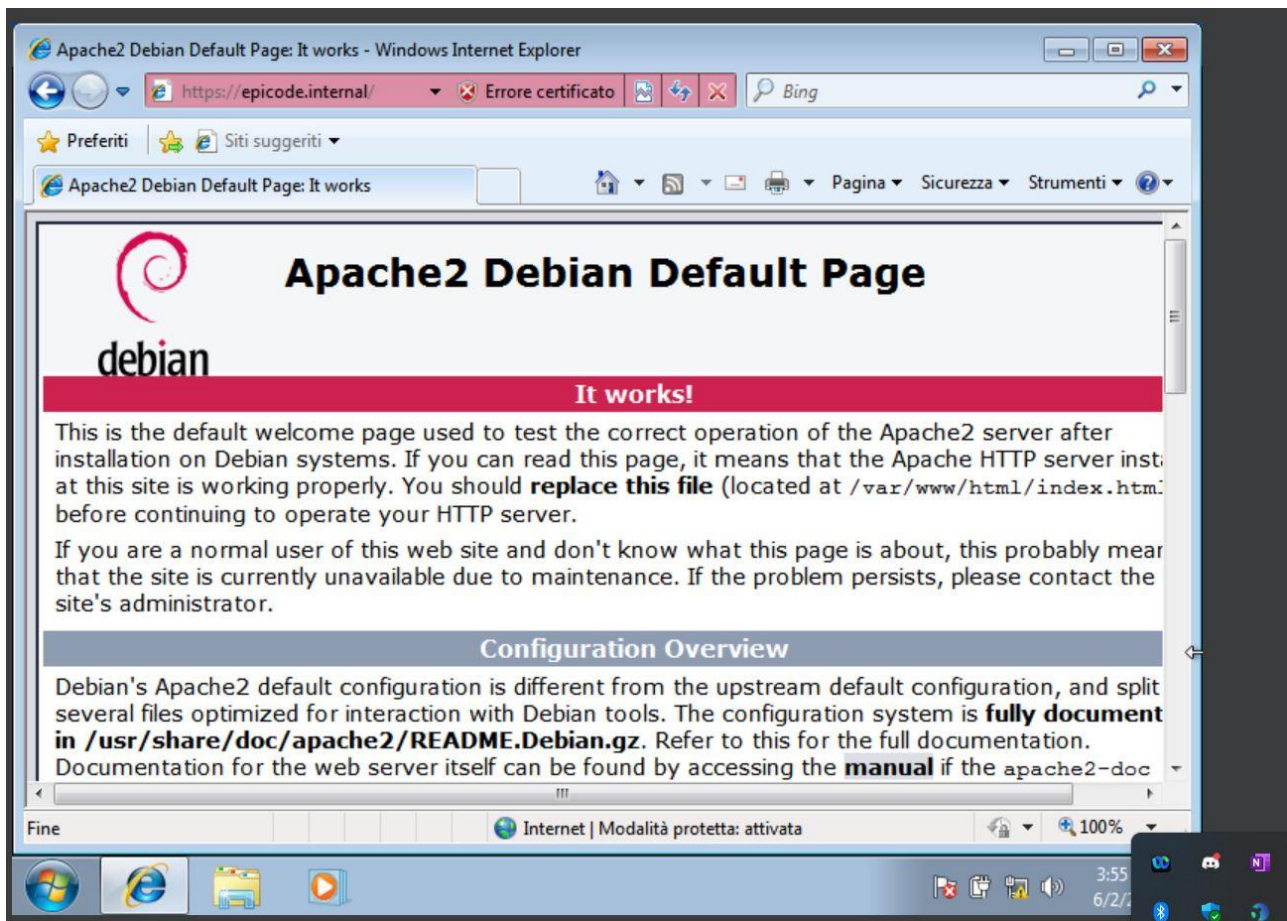
CREAZIONE DI UN NUOVO INDIRIZZO IP PER LA RETE KALI



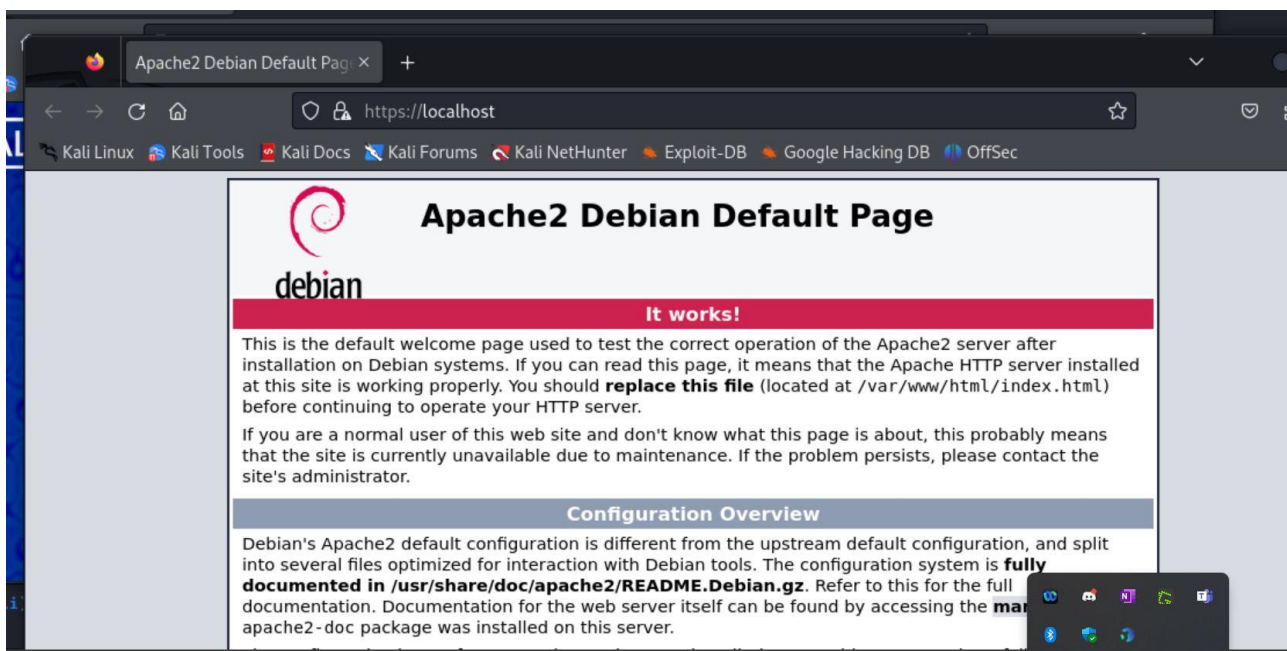
IMPOSTAZIONI DI RETE WINDOWS 7



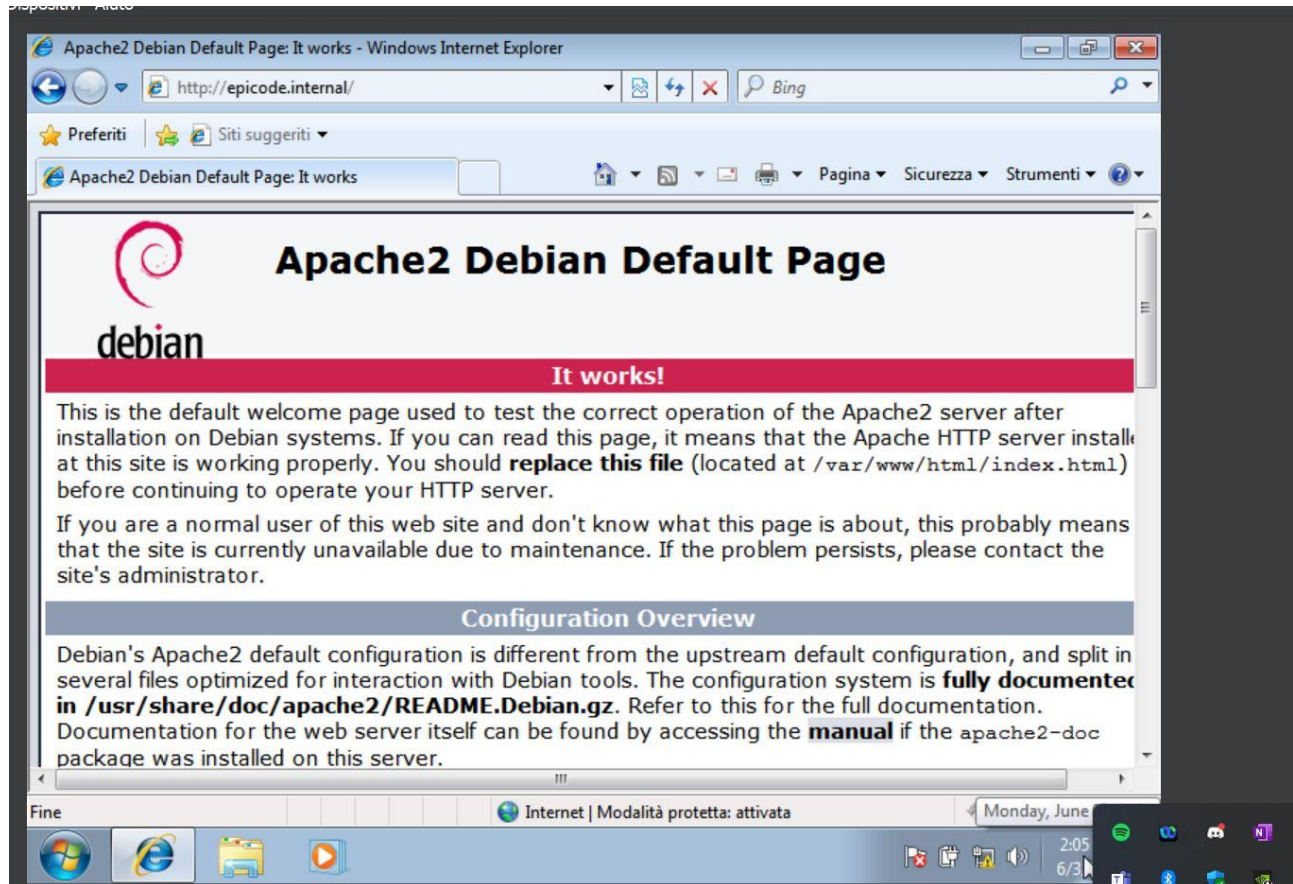
HTTPS WINDOWS 7



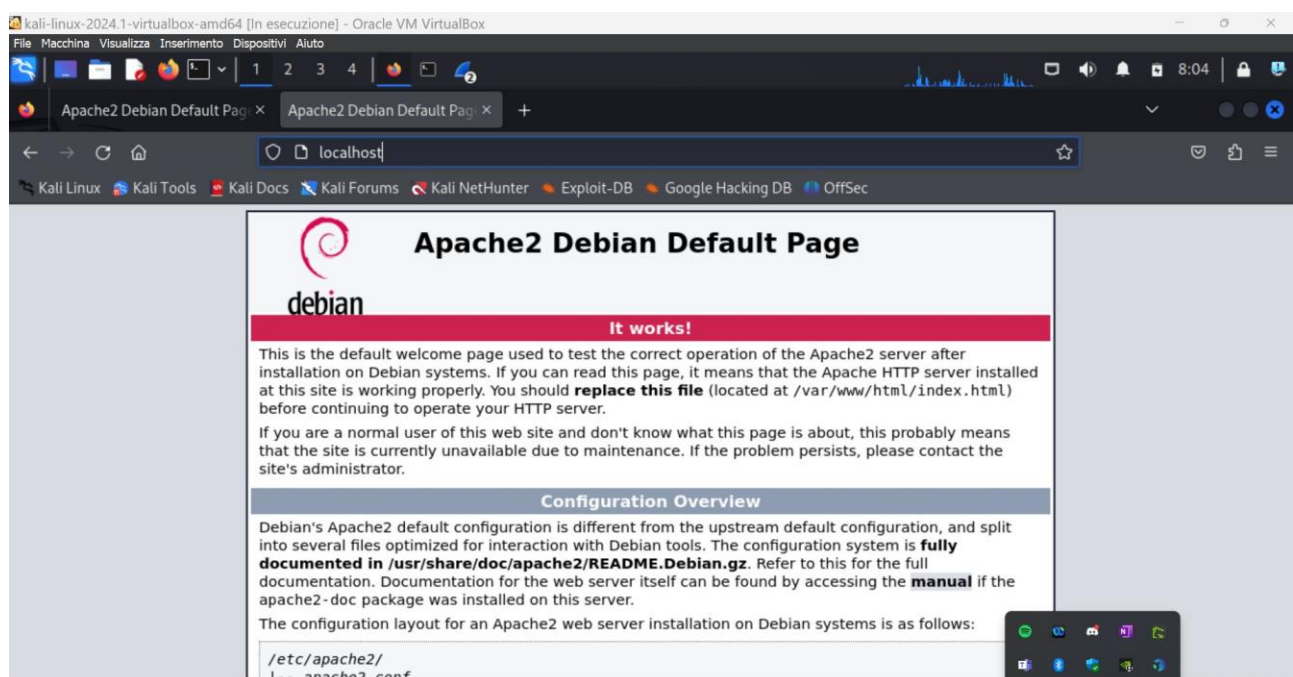
HTTPS KALI



HTTP WINDOWS 7



HTTP KALI



PACCHETTI http CON WIRESHARKE

The screenshot shows a Kali Linux virtual machine with Wireshark installed and running. The Wireshark interface is displaying a packet capture on the eth0 interface. The packet list pane shows five captured packets, all of which are HTTP requests from 192.168.32.100 to 192.168.32.100. The packet details pane shows the selected packet (No. 7) as a GET request for /icons/openlogo-75.png. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
7	83.953759937	192.168.32.100	192.168.32.100	HTTP	564	GET / HTTP/1.1
9	83.969610313	192.168.32.100	192.168.32.100	HTTP	3434	HTTP/1.1 200 OK (text/html)
11	83.979826368	192.168.32.100	192.168.32.100	HTTP	584	GET /icons/openlogo-75.png HTTP/1.1
12	83.986875962	192.168.32.100	192.168.32.100	HTTP	303	HTTP/1.1 304 Not Modified

Frame 7: 564 bytes on wire (4512 bits), 564 bytes captured (4512 bits) on eth0
 Ethernet II, Src: PCSystemtec_54:22:c7 (08:00:27:54:22:c7), Dst: PCSystemtec_54:22:c7 (08:00:27:54:22:c7)
 Destination: PCSystemtec_1e:36:4a (08:00:27:1e:36:4a)
 Source: PCSystemtec_54:22:c7 (08:00:27:54:22:c7)
 Type: IPv4 (0x0800)

Kali Linux - virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchine Visualizza Inserimento Dispositivi Aiuto

Wireshark - Packet 6 - eth0

- Frame 6: 3434 bytes on wire (27472 bits), 3434 bytes captured (27472 bits) on interface eth0, id 0
- Ethernet II, Src: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a), Dst: PCSSystemtec_54:22:c7 (08:00:27:54:22:c7)
 - Destination: PCSSystemtec_54:22:c7 (08:00:27:54:22:c7)
 - Address: PCSSystemtec_54:22:c7 (08:00:27:54:22:c7)
 - ... 0. = LG bit: Globally unique address (factory default)
 - ... 0. = IG bit: Individual address (unicast)
 - Source: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a)
 - Address: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a)
 - ... 0. = LG bit: Globally unique address (factory default)
 - ... 0. = IG bit: Individual address (unicast)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
- Transmission Control Protocol, Src Port: 80, Dst Port: 49174, Seq: 1, Ack: 400, Len: 3380
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - Date: Mon, 03 Jun 2024 12:25:06 GMT\r\n
 - Server: Apache/2.4.59 (Debian)\r\n
 - Last-Modified: Sun, 25 Feb 2024 15:55:18 GMT\r\n
 - ETag: "29cd-61236d1d67a20-gzip"\r\n
 - Accept-Ranges: bytes\r\n
 - Vary: Accept-Encoding\r\n
 - Content-Encoding: gzip\r\n
 - Content-Length: 3041\r\n
 - Keep-Alive: timeout=5, max=100\r\n
 - Connection: Keep-Alive\r\n
 - Content-Type: text/html\r\n

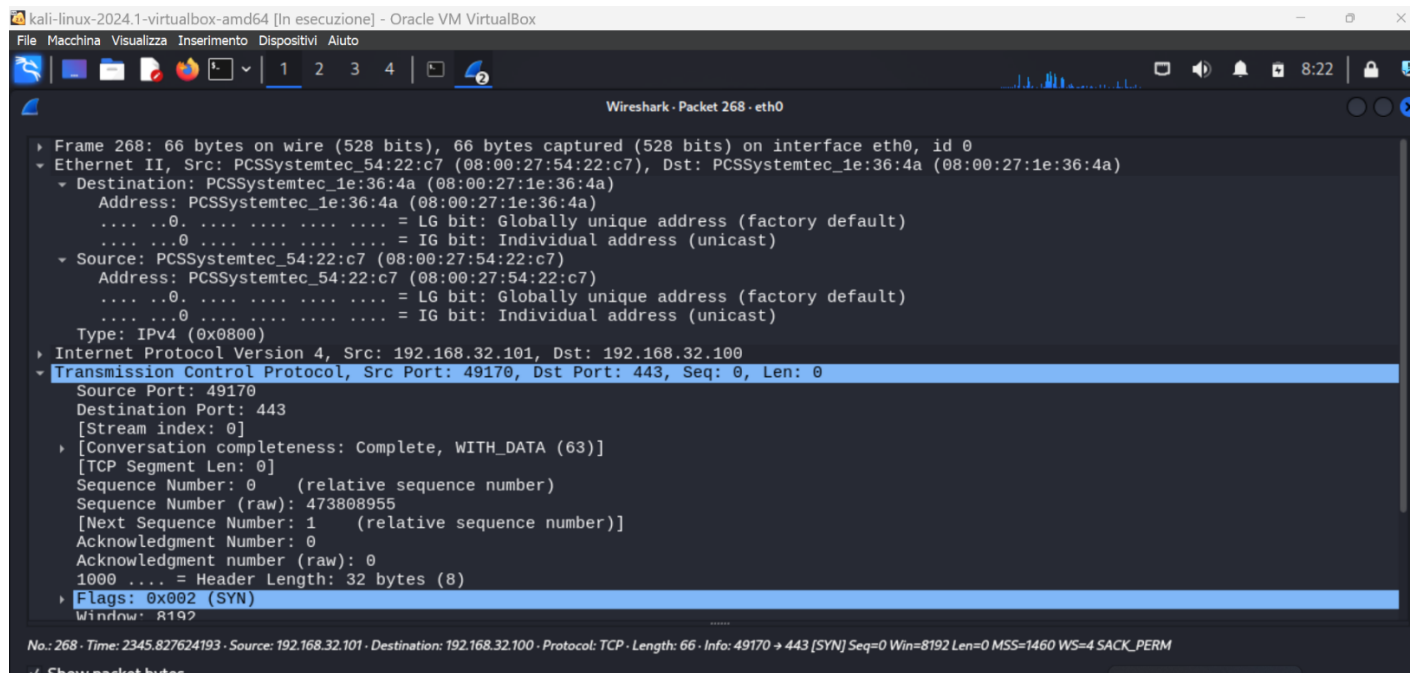
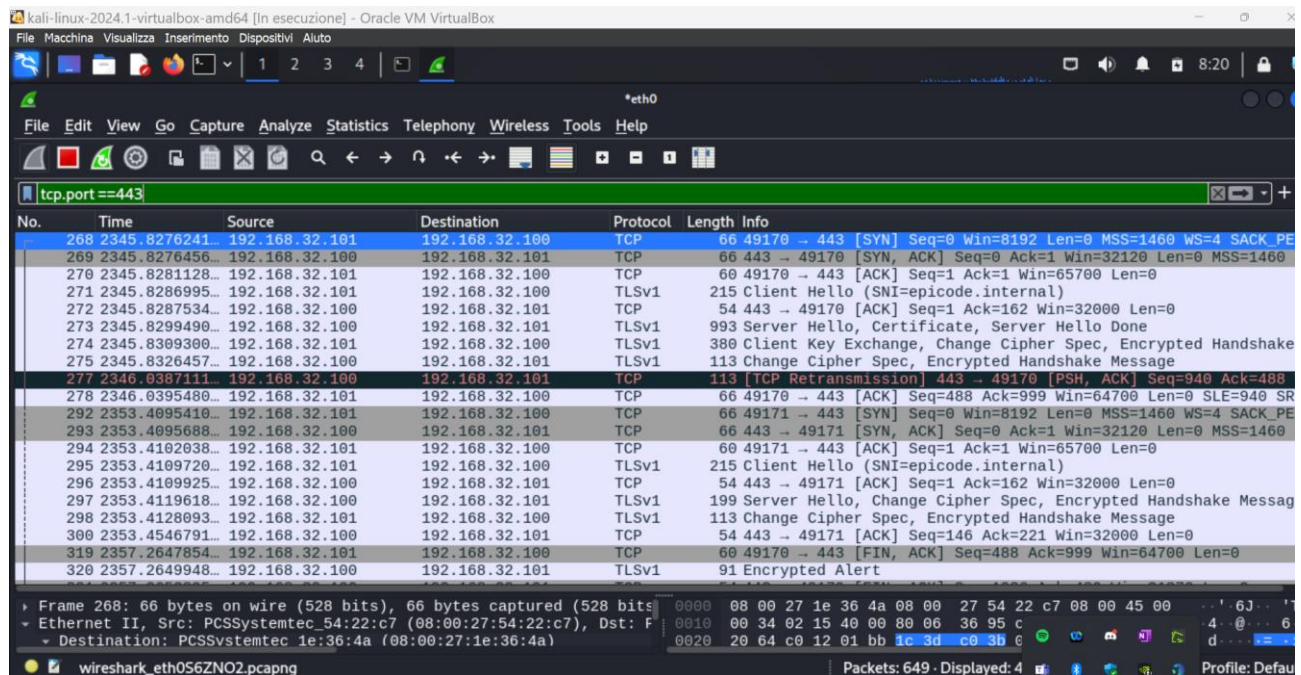
HTTP Date (http.date): 37 bytes

The image shows a Kali Linux terminal window with the title bar "Kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox". The terminal displays the output of the Wireshark packet capture tool, showing a packet list on the left and a packet details pane on the right. The packet list shows a single packet (Frame 4) of 453 bytes captured on interface eth0. The packet details pane shows the following information:

- Ethernet II, Src: PCSSystemtec_54:22:c7 (08:00:27:54:22:c7), Dst: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a)
- Destination: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a)
- Address: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
- Transmission Control Protocol, Src Port: 49174, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
- Hypertext Transfer Protocol
- GET / HTTP/1.1
- Accept: */*
- Accept-Language: en-US
- User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 1.1.4324.2282; .NET CLR 1.0.3705.6228)
- Accept-Encoding: gzip, deflate
- If-Modified-Since: Sun, 25 Feb 2024 15:55:18 GMT
- If-None-Match: "29cd-61236d1d67a20-gzip"
- Host: epicode.internal
- Connection: Keep-Alive
- Full request URI: http://epicode.internal/

The status bar at the bottom of the terminal window displays the following information: No: 4 - Time: 0.001475136 - Source: 192.168.32.101 - Destination: 192.168.32.100 - Protocol: HTTP - Length: 453 - Info: GET / HTTP/1.1

PACCHETTI HTTPS CON WIRESHARKE



DIFFERENZE TRA TRAFFICO HTTP E HTTPS

HTTP:

Le richieste e le risposte HTTP sono in chiaro e facilmente leggibili.

I dati possono essere intercettati e letti facilmente da chiunque nella rete.

Nessuna autenticazione garantita del server.

HTTPS:

Le richieste e le risposte HTTPS sono crittate. Solo il client e il server possono decifrare i dati.

I pacchetti HTTPS mostreranno dati crittografati e messaggi di handshake TLS.

HTTPS utilizza TLS/SSL per garantire la riservatezza e l'integrità dei dati.

Assicura che il server con cui il client sta comunicando è autentico (tramite certificati digitali).

Prima che i dati vengano trasmessi, HTTPS esegue un handshake TLS. Durante questo processo, il client e il server negoziano i parametri di crittazione.

I pacchetti di handshake TLS contengono dettagli sui certificati e le chiavi di sessione.

I MAC ADDRESS NON CAMBIANO QUANDO LA SORGENTE È LA STESSA